

Ручная установка SSL сертификата на сервер linux

Чтобы узнать какой веб-сервер обрабатывает SSL-запросы — Apache или Nginx, выполните команду:

```
netstat -napt | grep 443
```

Установка SSL-сертификата на Apache

Сертификат устанавливается в файле конфигурации Apache:

- для ОС Debian — **/etc/apache2/apache2.conf**;
- для ОС CentOS — **/etc/httpd/conf/httpd.conf**.

Добавьте данные о сертификате в секцию VirtualHost вашего домена:

Пример конфигурации

```
<VirtualHost 10.0.0.1:443>
  DocumentRoot /var/www/user/data/www/domain.com
  ServerName domain.com SSLEngine on
  SSLCertificateFile /path/to/domain.crt
  SSLCertificateKeyFile /path/to/domain.key
  SSLCACertificateFile /path/to/ca.crt
</VirtualHost>
```

Пояснения:

- domain.com — имя вашего домена
- 10.0.0.1 — IP-адрес, на котором находится домен
- **/var/www/user/data/www/domain.com** — путь до домашней директории вашего домена
- **/path/to/domain.crt** — файл, в котором находится сертификат

- **/path/to/domain.key** — файл, в котором находится ключ сертификата
- **/path/to/ca.crt** — файл корневого сертификата

Перезапустите Apache:

Команда для ОС CentOS

```
service httpd restart
```

или

```
systemctl restart httpd
```

Команда для ОС Debian/Ubuntu

```
service apache2 restart
```

или

```
systemctl restart apache2
```

Установка SSL-сертификата на Nginx

Сертификат устанавливается в файле конфигурации Nginx.

1.Объедините SSL-сертификат, промежуточный и корневой сертификаты в один файл **your_domain.crt**. Данные сертификатов вы можете найти в электронном сообщении, отправленным на ваш контактный e-mail после выпуска сертификата. Также вы можете скачать их вместе с основным сертификатом в личном кабинете на сайте planetahost.ru

Пример файла

```
-----BEGIN CERTIFICATE-----  
#Ваш сертификат#  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
#Промежуточный сертификат#  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
#Корневой сертификат#  
-----END CERTIFICATE-----
```

Обратите внимание!

Между сертификатами не должно быть пустых строк.

2.Создайте файл **your_domain.key** и скопируйте в него содержание приватного ключа сертификата.

3.Скопируйте файлы **your_domain.crt** и **your_domain.key** в одну директорию. Например, **/etc/ssl/**.

4.Настройте блок `server` в конфигурационном файле Nginx следующим образом:

```
server {  
    listen 443;  
    ssl on;  
    ssl_certificate /etc/ssl/your_domain.crt;  
    ssl_certificate_key /etc/ssl/your_domain.key;  
    server_name your.domain.com;  
}
```

Пояснения:

- **/etc/ssl/your_domain.crt** — путь к файлу с сертификатом
- **/etc/ssl/your_domain.key** — путь к файлу с приватным ключом сертификата
- **your.domain.com** — имя вашего домена

Обратите внимание!

Если нужно, чтобы сайт работал и с защищенным соединением по протоколу *https*, и с незащищенным по протоколу *http*, настройте два блока *server* для каждого типа соединения.

5.Перезагрузите сервер Nginx:

```
/etc/init.d/nginx restart
```

или

```
systemctl restart nginx
```

Версия #2

Кирилл создал 16 октября 2023 10:24:05

Кирилл обновил 16 октября 2023 13:17:09